

03S0914

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 Date of Application: 2002年12月27日

出願番号 Application Number: 特願2002-381380

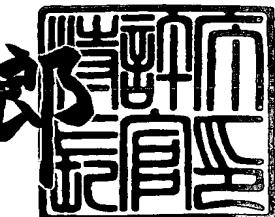
[ST. 10/C]: [JP2002-381380]

出願人 Applicant(s): 株式会社東芝

2003年 7月 8日

特許庁長官
Commissioner,
Japan Patent Office

太田信一



出証番号 出証特2003-3054008

【書類名】 特許願
【整理番号】 A000204959
【提出日】 平成14年12月27日
【あて先】 特許庁長官 殿
【国際特許分類】 G06F 15/00
【発明の名称】 電子透かし埋込装置、電子透かし検出装置、電子透かし埋込方法、電子透かし検出方法及びプログラム
【請求項の数】 24
【発明者】
【住所又は居所】 神奈川県川崎市幸区小向東芝町1番地 株式会社東芝研究開発センター内
【氏名】 村谷 博文
【特許出願人】
【識別番号】 000003078
【氏名又は名称】 株式会社 東芝
【代理人】
【識別番号】 100058479
【弁理士】
【氏名又は名称】 鈴江 武彦
【電話番号】 03-3502-3181
【選任した代理人】
【識別番号】 100084618
【弁理士】
【氏名又は名称】 村松 貞男
【選任した代理人】
【識別番号】 100068814
【弁理士】
【氏名又は名称】 坪井 淳

【選任した代理人】

【識別番号】 100092196

【弁理士】

【氏名又は名称】 橋本 良郎

【選任した代理人】

【識別番号】 100091351

【弁理士】

【氏名又は名称】 河野 哲

【選任した代理人】

【識別番号】 100088683

【弁理士】

【氏名又は名称】 中村 誠

【選任した代理人】

【識別番号】 100070437

【弁理士】

【氏名又は名称】 河井 将次

【手数料の表示】

【予納台帳番号】 011567

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 電子透かし埋込装置、電子透かし検出装置、電子透かし埋込方法、電子透かし検出方法及びプログラム

【特許請求の範囲】

【請求項 1】 透かし情報として入力された位相不变量に対応する第1の関数を生成する関数生成手段と、

入力された鍵情報に基づいて掛け混ぜ関数を生成し、該掛け混ぜ関数と前記第1の関数とを合成した第2の関数を計算する関数掛け混ぜ手段と、

入力された埋込対象コンテンツに対して前記第2の関数を埋め込む関数埋め込み手段とを備えたことを特徴とする電子透かし埋込装置。

【請求項 2】 前記第1の関数は、前記埋込対象コンテンツにおける埋め込む位置に関する基底空間から埋め込む量に関する対象空間への前記位相不变量に基づく写像を与える関数であることを特徴とする請求項1に記載の電子透かし埋込装置。

【請求項 3】 前記埋込対象コンテンツは、静止画像又は動画像データであり、

前記埋め込む位置に関する基底空間は、静止画像又は動画像データにおける画素位置のなす空間であり、

前記埋め込む量に関する対象空間は、静止画像又は動画像データにおける画素値に関する所定のベクトルのなす空間であることを特徴とする請求項1または2に記載の電子透かし埋込装置。

【請求項 4】 前記埋込対象コンテンツは、音声データであり、

前記埋め込む位置に関する基底空間は、音声データにおける時間的サンプリング位置のなす空間であり、

前記埋め込む量に関する対象空間は、音声データにおける振幅値に関する所定のベクトルのなす空間であることを特徴とする請求項1または2に記載の電子透かし埋込装置。

【請求項 5】 前記関数生成手段は、前記第1の関数を表現する第1の関数値を生成することを特徴とする請求項1ないし4のいずれか1項に記載の電子透

かし埋込装置。

【請求項 6】 前記関数搔き混ぜ手段は、前記関数生成手段により生成された前記第1の関数値に対して前記搔き混ぜ関数を適用して、前記第2の関数を表現する第2の関数値を生成することを特徴とする請求項5に記載の電子透かし埋込装置。

【請求項 7】 前記第1及び第2の関数値は、前記埋込対象コンテンツにおける各埋め込む位置に対する各埋め込む量を示すものであることを特徴とする請求項5または6に記載の電子透かし埋込装置。

【請求項 8】 前記関数搔き混ぜ手段は、前記鍵情報に基づくブロック暗号によって、前記第1の関数値を搔き混ぜて、前記第2の関数値を生成することを特徴とする請求項6または7に記載の電子透かし埋込装置。

【請求項 9】 前記関数埋め込み手段は、前記第2の関数値に基づいて前記埋込対象コンテンツの内容を変更することによって、前記位相不变量を埋め込むことを特徴とする請求項6ないし8のいずれか1項に記載の電子透かし埋込装置。

【請求項 10】 前記位相不变量は、ホモトピー不变量であることを特徴とする請求項1ないし9のいずれか1項に記載の電子透かし埋込装置。

【請求項 11】 入力された検出対象コンテンツに埋め込まれている第3の関数を検出する関数検出手段と、

入力された鍵情報に基づいて搔き混ぜ戻し関数を生成し、該搔き混ぜ戻し関数と前記第3の関数を合成した第4の関数を計算する関数搔き混ぜ戻し手段と、

前記第4の関数に基づいて透かし情報としての位相不变量を計算する位相不变量計算手段とを備えたことを特徴とする電子透かし検出装置。

【請求項 12】 前記第4の関数は、前記埋込対象コンテンツにおける埋め込む位置に関する基底空間から埋め込む量に関する対象空間への前記位相不变量に基づく写像を与える関数であることを特徴とする請求項11に記載の電子透かし検出装置。

【請求項 13】 前記埋込対象コンテンツは、静止画像又は動画像データであり、

前記埋め込む位置に関する基底空間は、静止画像又は動画像データにおける画素位置のなす空間であり、

前記埋め込む量に関する対象空間は、静止画像又は動画像データにおける画素値に関する所定のベクトルのなす空間であることを特徴とする請求項11または12に記載の電子透かし検出装置。

【請求項14】 前記埋込対象コンテンツは、音声データであり、

前記埋め込む位置に関する基底空間は、音声データにおける時間的サンプリング位置のなす空間であり、

前記埋め込む量に関する対象空間は、音声データにおける振幅値に関する所定のベクトルのなす空間であることを特徴とする請求項11または12に記載の電子透かし検出装置。

【請求項15】 前記関数検出手段は、前記第3の関数を表現する第3の関数値を検出することを特徴とする請求項11ないし14のいずれか1項に記載の電子透かし検出装置。

【請求項16】 前記関数搔き混ぜ戻し手段は、前記関数検出手段により検出された前記第3の関数値に対して前記搔き混ぜ戻し関数を適用して、前記第4の関数を表現する第4の関数値を生成することを特徴とする請求項15に記載の電子透かし検出装置。

【請求項17】 前記第3及び第4の関数値は、前記埋込対象コンテンツにおける各埋め込む位置に対する各埋め込む量を示すものであることを特徴とする請求項15または16に記載の電子透かし検出装置。

【請求項18】 前記関数搔き混ぜ戻し手段は、前記鍵情報に基づくブロック暗号によって、前記第3の関数値を搔き混ぜ戻して、前記第4の関数値を生成することを特徴とする請求項16または17に記載の電子透かし検出装置。

【請求項19】 前記第4の関数は、前記埋込対象コンテンツにおける埋め込む位置に関する基底空間から埋め込む量に関する対象空間への前記位相不变量に基づく写像を与える関数であって、該写像を決定付けるパラメータとして前記位相不变量によるパラメータを持つものであり、

前記位相不变量計算手段は、前記第4の関数値に基づいて前記写像を決定付け

るパラメータを求めるこことによって、前記位相不变量を計算することを特徴とする請求項16ないし18のいずれか1項に記載の電子透かし検出装置。

【請求項20】 前記位相不变量は、ホモトピー不变量であることを特徴とする請求項11ないし19のいずれか1項に記載の電子透かし検出装置。

【請求項21】 透かし情報として入力された位相不变量に対応する第1の関数を生成する関数生成ステップと、

入力された鍵情報に基づいて掛け混ぜ関数を生成し、該掛け混ぜ関数と前記第1の関数とを合成した第2の関数を計算する関数掛け混ぜステップと、

入力された埋込対象コンテンツに対して前記第2の関数を埋め込む関数埋め込みステップとを有することを特徴とする電子透かし埋込方法。

【請求項22】 入力された検出対象コンテンツに埋め込まれている第3の関数を検出する関数検出ステップと、

入力された鍵情報に基づいて掛け混ぜ戻し関数を生成し、該掛け混ぜ戻し関数と前記第3の関数を合成した第4の関数を計算する関数掛け混ぜ戻しステップと

前記第4の関数に基づいて透かし情報としての位相不变量を計算する位相不变量計算ステップとを有することを特徴とする電子透かし検出方法。

【請求項23】 コンピュータを電子透かし埋込装置として機能させるためのプログラムであって、

透かし情報として入力された位相不变量に対応する第1の関数を生成する関数生成機能と、

入力された鍵情報に基づいて掛け混ぜ関数を生成し、該掛け混ぜ関数と前記第1の関数とを合成した第2の関数を計算する関数掛け混ぜ機能と、

入力された埋込対象コンテンツに対して前記第2の関数を埋め込む関数埋め込み機能とをコンピュータに実現させるためのプログラム。

【請求項24】 コンピュータを電子透かし検出装置として機能させるためのプログラムであって、

入力された検出対象コンテンツに埋め込まれている第3の関数を検出する関数検出機能と、

入力された鍵情報に基づいて掛け混ぜ戻し関数を生成し、該掛け混ぜ戻し関数と前記第3の関数を合成した第4の関数を計算する関数掛け混ぜ戻し機能と、

前記第4の関数に基づいて透かし情報としての位相不变量を計算する位相不变量計算機能とをコンピュータに実現させるためのプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、デジタル・データ化された静止画データ、動画データ、音声データ、音楽データ等のコンテンツに対して透かし情報を埋め込む電子透かし埋込装置及び電子透かし埋込方法、コンテンツから透かし情報を検出する電子透かし検出装置及び電子透かし検出方法、並びにプログラムに関する。

【0002】

【従来の技術】

(電子透かし)

電子透かし (digital watermarking) は、デジタルデータ化された静止画、動画、音声、音楽等のデジタル・コンテンツ (あるいは、デジタル著作物データ) に対して、品質劣化が目立たない程度の小さな変更を加えることで別の情報を埋め込む技術である。例えば、コンテンツの著作権者の識別情報、コンテンツの利用者の識別情報、コンテンツの著作権者の権利情報、コンテンツの利用条件、コンテンツの利用時に必要な秘密情報、コピー制御情報などの情報(以下、透かし情報と呼ぶ)を知覚が容易ではない状態となるように埋め込み、後に必要に応じて透かし情報をコンテンツから検出することによって利用制御、コピー制御を含む著作権保護を行ったり、二次利用の促進を行うものである。また、例えば、著作者の識別、所有権の証明、フィンガープリンティング、コンテンツの証明、放送の監視などの応用が提案されている。

【0003】

(電子透かしの要件)

デジタル・コンテンツの不正利用の防止を目的とする場合、透かし情報は、そのコンテンツに対して通常に施されると想定される各種の操作や意図的な攻撃に

よって、消失したり改ざんされたりしないような性質（robustness：ロバスト性）を持つ必要がある。

【0004】

(幾何学的改変)

デジタル・コンテンツが画像（静止画や動画）の場合、幾何学的変形によって、電子透かしを消失させる攻撃がある。幾何学的変形とは、画像の座標変換である。幾何学的変形は、画素の位置を変えてしまうため、電子透かしの方式によつては、検出時に、画素の位置の同期がとれずに、正しく透かし情報が読み取れないという問題が生ずる。

【0005】

幾何学的変形は、2つに大別される。大域的変形と局所的変形である。大域的変形は、画像全体のスケーリング、回転、平行移動であり、アフィン変換として表現される。一方、局所的変換は、大域的変換のように位置によらないパラメータによって表現される変形だけでなく、局所的なパラメータによって表現される変換を含む変換である。大域的変換は、局所的変換の特殊な場合である。

【0006】

(位相的電子透かし方式)

同相な空間には、位相不变量と呼ばれる不变な性質が存在し得ることが知られている。例えば、ホモトピー類がその例である（例えば、非特許文献1参照）。

【0007】

そこで、局所的な幾何学的変形を同相写像とみなすことで、電子透かしを位相不变量と関連付けることが考えられる。この局所的な幾何学的変形に対するロバスト性を実現するための技術として、位相的電子透かし方式がある（例えば、特許文献1参照）。位相的電子透かし方式は、局所的な幾何学的変形の下で不变な位相不变量（例えば、ホモトピー類）を電子透かしとして埋め込む。電子透かしは、所定のホモトピー類 b に属する関数 Ψ_b によって表現されて埋め込まれる。電子透かしの検出は、検出された関数 Ψ_b' からそのホモトピー類 b を計算することを行われる。

【0008】

【特許文献1】

特開2002-142094

【0009】

【非特許文献1】

岩波数学辞典第3版, 位相空間, 22-34, ホモトピー理論, 1142-1

150

【0010】

【発明が解決しようとする課題】

従来の電子透かし技術では、電子透かしを位相不変量としてコンテンツに埋め込むにあたって、素直な埋め込み方をしていた。

【0011】

本発明は、上記事情を考慮してなされたもので、S t i r M a r k 攻撃やD-A-D変換などの局所的変形に対する耐性を持つとともに、電子透かしのアルゴリズムの全部又は一部が開示されたとしてもなお安全であるような電子透かし埋込装置及び電子透かし検出装置、電子透かし埋込方法及び電子透かし検出方法、並びにプログラムを提供することを目的とする。

【0012】

【課題を解決するための手段】

本発明に係る電子透かし埋込装置は、透かし情報として入力された位相不変量に対応する第1の関数を生成する関数生成手段と、入力された鍵情報に基づいて掻き混ぜ関数を生成し、該掻き混ぜ関数と前記第1の関数とを合成した第2の関数を計算する関数掻き混ぜ手段と、入力された埋込対象コンテンツに対して前記第2の関数を埋め込む関数埋め込み手段とを備えたことを特徴とする。

【0013】

また、本発明に係る電子透かし検出装置は、入力された検出対象コンテンツに埋め込まれている第3の関数を検出する関数検出手段と、入力された鍵情報に基づいて掻き混ぜ戻し関数を生成し、該掻き混ぜ戻し関数と前記第3の関数を合成した第4の関数を計算する関数掻き混ぜ戻し手段と、前記第4の関数に基づいて透かし情報としての位相不変量を計算する位相不変量計算手段とを備えたことを

特徴とする。

【0014】

好ましくは、前記第1、第4の関数は、前記埋込対象コンテンツにおける埋め込む位置に関する基底空間から埋め込む量に関する対象空間への前記位相不变量に基づく写像を与える関数であるようにしてもよい。

【0015】

好ましくは、前記第1～第4の関数値は、前記埋込対象コンテンツにおける各埋め込む位置に対する各埋め込む量を示すものであるようにしてもよい。

【0016】

好ましくは、前記関数焼き混ぜ手段は、前記鍵情報に基づくブロック暗号によって、前記第1の関数値を焼き混ぜて、前記第2の関数値を生成するようにしてもよい。

【0017】

好ましくは、前記関数焼き混ぜ戻し手段は、前記関数検出手段により検出された前記第3の関数値に対して前記焼き混ぜ戻し関数を適用して、前記第4の関数を表現する第4の関数値を生成するようにしてもよい。

【0018】

なお、装置に係る本発明は方法に係る発明としても成立し、方法に係る本発明は装置に係る発明としても成立する。

また、装置または方法に係る本発明は、コンピュータに当該発明に相当する手順を実行させるための（あるいはコンピュータを当該発明に相当する手段として機能させるための、あるいはコンピュータに当該発明に相当する機能を実現させるための）プログラムとしても成立し、該プログラムを記録したコンピュータ読取り可能な記録媒体としても成立する。

【0019】

本発明では、対象となるデジタル・コンテンツ（例えば、画像データ）に透かし情報を埋め込む際、対象コンテンツに埋め込むべき透かし情報に対応する所定の位相不变量（例えば、ホモトピー不变量）を得て、対象コンテンツの内容のうち予め定められた部分を変更することによって、該コンテンツに該位相不变量を

設定する。

また、本発明では、対象となるデジタル・コンテンツから該コンテンツに埋め込まれた透かし情報を検出する際、対象コンテンツの内容のうち予め定められた部分に基づいて、該コンテンツに設定された所定の位相不变量を検出し、検出された該所定の位相不变量に対応する透かし情報を出力する。

例えば、透かし情報としてコピー可を指示する制御情報を埋め込む際に、例えばホモトピー類の全体が整数全体 \mathbb{Z} と同型である場合に、ホモトピー類 $= +1$ （もちろん、 $+1$ 以外の値でもよい）となるように画素値を変更し、コピー不可とする場合に、ホモトピー類 $= -1$ （もちろん、 -1 以外の値でもよい）となるように画素値を変更する。また、例えば、透かし情報として著作権者等の識別番号を埋め込む場合に、識別番号1が指定されたならば、ホモトピー類 $= 1$ （もちろん、 1 以外の値でもよい）となるように画素値を変更し、識別番号2が指定されたならば、ホモトピー類 $= 2$ （もちろん、 2 以外の値でもよい）となるように画素値を変更する。

【0020】

本発明によれば、埋め込むべき透かし情報に対応する位相不变量を対象コンテンツに設定するようにしたので、たとえ流通経路などでStirMark攻撃やD-A-D-変換などの局所的変形を受けてもコンテンツに設定した位相不变量は維持・保存される。そして、局所的変形を受けたか否かにかかわらずコンテンツから正しい位相不变量を検出し、対応する正しい透かし情報を得ることができる。

【0021】

また、コンテンツのビット列の変化が小さくなるように位相不变量を表現するデータを書き込むことによって、なるべくコンテンツに影響を与えないようにすることができる。

【0022】

これに加えて、本発明では、埋め込み時には、第1の関数（値）を埋め込むのではなく、第1の関数（値）に対して鍵情報に基づく掛け混ぜを行った後に、これによって得られた第2の関数（値）を埋め込むので、検出時には、第3の関数

(値) から位相不变量を求ることはできず、埋め込み時に用いた鍵情報に対応する鍵情報があつてはじめて、該鍵情報に基づく搔き混ぜ戻しを行った後に、これによって得られた第4の関数(値)（鍵情報が正しければ、第4の関数(値) = 第1の関数(値)となる）をもとにして、正しい位相不变量を得ることができる。第3の関数(値)からは、電子透かしの存在自体を知ることも難しく、それを知っていたとしても、正しい位相不变量を得ることはできず、また、正しい鍵情報がなければ、第4の関数(値)からも正しい位相不变量を求ることはできない。

【0023】

なお、本発明では、鍵情報に基づく搔き混ぜ及び搔き混ぜ戻しは、従来の単なるスクランブル及びデスクランブルではない。従来のように単純に画像をスクランブルした後に、幾何学的改変を受けると、デスクランブルして元に戻せなくなることがあるが、本発明によれば、鍵情報に基づく搔き混ぜを行った後に、幾何学的改変を受けても、鍵情報に基づく搔き混ぜ戻しができるようになっている。

【0024】

このように、本発明によれば、StirMark攻撃やD-A-D-変換などの局所的変形に対する耐性を持つとともに、電子透かしのアルゴリズムの全部又は一部が開示されたとしてもなお安全であるような電子透かしを実現することができる。

【0025】

【発明の実施の形態】

以下、図面を参照しながら発明の実施の形態を説明する。

【0026】

本発明は、コンテンツ（例えば、デジタルデータ化された静止画、動画、音声、音楽等）に対して様々な透かし情報（例えば、コンテンツの著作権者や利用者の識別情報、著作権者の権利情報、コンテンツの利用条件、その利用時に必要な秘密情報、コピー制御情報等、あるいはそれらを組み合わせたものなど）を様々な目的（例えば、利用制御、コピー制御を含む著作権保護、二次利用の促進等）で埋め込み、検出する場合に適用可能である。

【0027】

図1に、本発明の一実施形態に係る電子透かし埋込装置と電子透かし検出装置が適用されるシステムの概念図を示す。

【0028】

電子透かし埋込装置1は、埋め込み対象となるコンテンツに透かし情報を埋め込むもので、対象コンテンツとこれに埋め込むべき透かし情報と鍵情報が入力され、電子透かし情報埋め込み済みコンテンツを出力する。電子透かし埋込装置1は、コンテンツ提供側に備えられ、管理される。

【0029】

電子透かし埋込装置1により得られた電子透かし情報埋め込み済みコンテンツは、記憶媒体や通信媒体などを媒介とした流通経路3を経て流通する。その際、流通経路3では、コンテンツに対してStirMark攻撃やD-A-D変換などの局所的変換がなされることがある（局所的変換は、ユーザの故意によってなされることもあるし、ユーザの故意あるいは認識なくしてなされることもある）。

【0030】

電子透かし検出装置2は、検出対象となるコンテンツから透かし情報を検出するもので、対象コンテンツと鍵情報が入力され、検出された透かし情報を出力する。電子透かし検出装置2は、コンテンツ利用時の著作権保護を目的としてユーザ側のコンテンツ利用装置に内蔵される場合や、コンテンツ提供側が流通を経たコンテンツから電子透かしを検出することを目的としてコンテンツ提供側に備えられる場合がある。

【0031】

本実施形態では、詳しくは後述するように、電子透かし埋込装置1は、StirMark攻撃やD-A-D変換などがなされても透かし情報の内容が維持・保存されるように透かし情報を埋め込むので、流通経路3においてコンテンツに対してStirMark攻撃やD-A-D変換などがなされても、電子透かし検出装置2は、電子透かし埋込装置1で埋め込まれた透かし情報を正しく検出することができる。

【0032】

また、電子透かし検出装置2は、電子透かし埋込装置1で当該コンテンツについて使用した鍵情報に対応する正当な鍵情報（例えば、共通鍵暗号方式が用いられる場合には、電子透かし埋込装置1で使用した鍵情報と同一の鍵情報）を用いることによってのみ、当該コンテンツに埋め込まれた透かし情報を正しく検出することができるので、電子透かしのアルゴリズムが開示されたとしても鍵情報が開示されていなければ安全であるように構成することができるものとなっている。

【0033】

なお、本実施形態では、電子透かし埋込装置1にはデジタル・コンテンツが入力され、電子透かし検出装置2からはデジタル・コンテンツが出力されるものとして説明するが、電子透かし埋込装置1に、入力されたアナログ・コンテンツを透かし情報の埋め込みに先立ってデジタル・コンテンツに変換する機能を搭載してもよいし、およびまたは、電子透かし検出装置2に、入力されたアナログ・コンテンツを透かし情報の検出に先立ってデジタル・コンテンツに変換する機能を搭載してもよい。

【0034】

電子透かし埋込装置1は、ソフトウェア（プログラム）としてもハードウェアとしても実現可能である。同様に、電子透かし検出装置2は、ソフトウェア（プログラム）としてもハードウェアとしても実現可能である。

電子透かし埋込装置1および電子透かし検出装置2をコンテンツ提供側で用いる場合には、それらを一体化して実現することも可能である。

電子透かし検出装置2をユーザ側のコンテンツ利用装置に内蔵する場合には、ユーザにより電子透かし検出装置2に対する操作や解析あるいは攻撃などができるないように安全に作り込んでおくのが望ましい。

【0035】

なお、以下で示す構成図は、装置の機能ブロック図としても成立し、また、ソフトウェア（プログラム）の機能モジュール図あるいは手順図としても成立するものである。

【0036】

本実施形態では、デジタル・コンテンツの一例として主に動画像データを対象とした場合を例にとって説明するが、静止画像データや音声データ等の他のメディアのデータを対象とすることも可能である。なお、StirMark攻撃やD-A-D変換などの局所的変形は、例えば、動画像については、フレーム単位で処理する場合には、データの幾何学的変形であり、複数フレームにわたって時間的位置を考慮して処理する場合にはデータの幾何学的変形および時間軸方向の変形（時空間的変形）である。また、静止画の場合には、静止画データの幾何学的変形であり、音声の場合には、音声データの時間軸方向の変形である。

【0037】

さて、本実施形態は、透かし情報を位相不变量（topological invariant）としてコンテンツに埋め込む（例えば対象コンテンツから得られる位相不变量が透かし情報に対応する値になるように対象コンテンツの画素値等を操作する）ことによって、StirMark攻撃やD-A-D変換などの局所的変形に対して耐性を持つようにしたものであるが、以下では、電子透かしとして位相不变量を直接用いる場合を例にとって説明するものとし、また、位相不变量の一例としてホモトピー不变量（homotopy invariant）を用いた構成例について説明する。

【0038】

なお、電子透かしとして位相不变量を直接用いる代わりに、電子透かし埋込装置1側に、与えられた透かし情報を埋め込むべき位相不变量に変換する透かし情報・位相不变量変換部を設け、電子透かし検出装置2側に、検出された位相不变量を対応する透かし情報に変換する位相不变量・透かし情報変換部を設けるようにしてもよい。

【0039】

また、位相不变量やホモトピー不变量やホモトピー類などの電子透かしへの応用については、特許文献1に開示されたものと同様の考え方を用いることができる。

【0040】

図2に、本発明の一実施形態に係る電子透かし埋込装置の構成例を示す。

【0041】

本電子透かし埋込装置は、埋め込み対象のデジタルコンテンツ（本例では、動画像）と、埋め込むべき電子透かしであるホモトピー類と、鍵情報とを入力として、電子透かしの埋め込み済みコンテンツを出力する。

【0042】

図2に示されるように、本電子透かし埋込装置は、関数生成部11、関数掻き混ぜ部12、関数埋め込み部13を備えている。

【0043】

図3に、本実施形態の電子透かし埋込装置の処理手順の一例を示す。

電子透かしを埋め込む対象となる埋め込み対象画像、鍵情報、透かし情報（本例では、ホモトピー類）を入力する（ステップS1）。

与えられたホモトピー類に属する関数を生成する（ステップS2）。

与えられた鍵情報に従い、掻き混ぜ関数を生成し、上記のホモトピー類に属する関数との合成関数を生成する（ステップS3）。

生成された合成関数を埋め込み対象画像に埋め込む（ステップS4）。

電子透かしを埋め込まれた埋め込み済み画像を出力する（ステップS5）。

【0044】

まず、関数生成部11の機能について説明する。

【0045】

ここで、画像は、画素の集まりである。

【0046】

画素は、画像中の位置と、その位置における色によって、記述される。

【0047】

画像中の位置のなす空間Bを基底空間、色の空間Cを色空間と呼ぶ。例えば、静止画あるいは動画の1フレームの場合には、基底空間Bは、2次元の有限領域である。カラー画像の場合には、色空間Cは、3次元の有限領域である。

【0048】

n個（n≥1とする）の色空間Cの積空間Cⁿ=C×C×…×Cの中に所定の

部分空間 $T \subset C^n$ を構成し、それを対象空間と呼ぶことにする。色空間 C の中に対象空間 T を包含する所定の部分空間 $S \subset T$ を設定してあるものとし、これを掻き混ぜ空間と呼ぶ。

【0049】

本例では、基底空間 B の同相写像に対する不变量を透かし情報とみなす。具体的には、位相不变量として、基底空間 B から対象空間 T への写像が属するホモトピー類を利用する。

【0050】

関数生成部 1 1 は、埋め込むべき情報であるところのホモトピー類 b が入力されたとき、それに属する関数 $\Psi_b : B \rightarrow T$ を生成する。

【0051】

次に、関数掻き混ぜ部 1 2 の機能について説明する。

【0052】

関数掻き混ぜ部 1 2 は、掻き混ぜ空間 S から掻き混ぜ空間 S への写像であって、入力される鍵情報 k に応じて異なる関数（掻き混ぜ関数） $g_k : S \rightarrow S$ を生成し、この鍵情報 k に基づく掻き混ぜ関数 g_k と、関数生成部 1 1 が生成したホモトピー類 b に属する関数 Ψ_b との合成関数 $g_k \circ \Psi_b : B \rightarrow S$ を生成する（なお、 \circ は、その前後に記述された関数の合成関数を表すものとする）。

【0053】

次に、関数埋め込み部 1 3 の機能について説明する。

【0054】

関数埋め込み部 1 3 は、関数掻き混ぜ部 1 2 が生成した合成関数 $g_k \circ \Psi_b$ を、埋め込み対象画像に埋め込む。埋め込みは、基底空間 B の各点に対して、掻き混ぜ空間 S 中の値が、合成関数の与える値となるように、画像を変更することによって、実施する。そして、電子透かしを埋め込んだ対象画像を埋め込み済み画像として出力する。

【0055】

図 4 に、本発明の一実施形態に係る電子透かし検出装置の構成例を示す。

【0056】

本電子透かし検出装置は、検出対象のコンテンツ（本例では、動画像）と、鍵情報とを入力として、電子透かし情報であるホモトピー類を出力する。

【0057】

図4に示されるように、本電子透かし検出装置は、関数検出部21、関数掻き混ぜ戻し部22、ホモトピー類計算部23を備えている。

【0058】

図5に、電子透かし検出装置の処理手順の一例を示す。

電子透かしを検出する対象となる検出対象画像、鍵情報を入力する（ステップS11）。

検出対象画像から、埋め込まれている関数を読み取る（ステップS12）。

【0059】

与えられた鍵情報に従い、（前記の掻き混ぜ関数に対応する）掻き混ぜ戻し関数を生成し、上記の埋め込まれている関数との合成関数を生成する（ステップS13）。

生成された合成関数の属するホモトピー類を計算する（ステップS14）。

求められたホモトピー類を電子透かしとして出力する（ステップS15）。

【0060】

まず、関数検出部21の機能について説明する。

【0061】

関数検出部21は、検出対象画像が与えられたとき、その画像から、基底空間Bの各点に対する掻き混ぜ空間Sにおける値を求めるこことによって、埋め込まれている関数 $\Phi: B \rightarrow S$ を求める。

【0062】

次に、関数掻き混ぜ戻し部22の機能について説明する。

【0063】

関数掻き混ぜ戻し部22は、関数掻き混ぜ部12と同様に、掻き混ぜ空間Sから掻き混ぜ空間Sへの写像であって、入力される鍵情報kに応じて異なる関数 $g_k^{-1}: S \rightarrow S$ を生成する。この g_k^{-1} は、先の g_k の逆となっている。すなわち、 $g_k^{-1} \circ g_k = 1$ である。

【0064】

関数掻き混ぜ戻し部22は、さらに、この鍵情報kに基づく掻き混ぜ戻し関数 g_k^{-1} と、関数生成部11が生成した埋め込まれている関数 Φ との合成関数 $g_k^{-1} \circ \Phi : B \rightarrow S$ を生成する。

【0065】

検出対象が、電子透かしを埋め込まれた画像であって、関数掻き混ぜ戻し部22が、電子透かし埋込装置1の関数掻き混ぜ部12が用いた鍵情報と同じ鍵情報kを用いるときは、関数掻き混ぜ戻し部22により生成された合成関数 $\Xi : B \rightarrow S$ は、 $\Xi = g_k^{-1} \circ \Phi = g_k^{-1} \circ g_k \circ \Psi_b = \Psi_b$ となる。この Ψ_b は、電子透かし埋込装置1の関数生成部11が生成した、電子透かしとして与えられたホモトピー類bに属する関数（ $\Psi_b : B \rightarrow T$ ）である。従って、この合成関数 Ξ の値域は、対象空間T上にあることが期待される。つまり、 $\Xi : S \rightarrow T$ である。

【0066】

関数掻き混ぜ戻し部22が、当該検出対象画像について電子透かし埋込装置1の関数掻き混ぜ部12が用いた鍵情報とは異なる鍵情報 k' を用いるときは、 $\Xi' = g_{k'}^{-1} \circ \Phi = g_{k'}^{-1} \circ g_k \circ \Psi_b$ となって、一般的には、 $\Xi' \neq \Psi_b$ となり、合成関数 Ξ' の値域は、T上に収まる保障がない。よって、対象となったコンテンツが、電子透かしが埋め込まれた画像であるか否かを知ることは難しいし、正しい Ξ を知ることも（従って、埋め込まれている電子透かしの正しい内容を知ることも）難しい。

【0067】

次に、ホモトピー類計算部23の機能について説明する。

【0068】

ホモトピー類計算部23の機能は、関数掻き混ぜ戻し部22により得られた合成関数 $\Xi : B \rightarrow T$ から、その合成関数の属するホモトピー類を計算する。そして、その結果を、得られた電子透かしとして出力する。

【0069】

なお、ここでは、同一のコンテンツについて、電子透かし埋込装置1で用いる掻き混ぜ関数を決定付ける鍵情報と電子透かし検出装置2で用いる掻き混ぜ戻し

関数を決定付ける鍵情報とを同一のものとする場合を例にとって説明しているが、電子透かし埋込装置1で生成する掻き混ぜ関数と、電子透かし検出装置2で生成する掻き混ぜ戻し関数とが、逆になるようにできさえすれば、電子透かし埋込装置1で用いる鍵情報と、電子透かし検出装置2で用いる鍵情報とが同一でないような構成にしてもよい。

【0070】

以下、具体例を用いて本実施形態について説明する。

【0071】

画像中の画素の位置のなす空間である基底空間Bは、本来は、例えば、縦512画素、横512画素からなるような、2次元有限領域であるが、この基底空間Bの周囲を1点と同一視するように変形することで、基底空間Bを2次元球面S²であるとみなすことができる。この様子を、図6に示す。

【0072】

この同一視により、基底空間Bの座標を、2次元球面の極座標 (θ, ϕ) で表すことができる。ここで、 $\theta \in [0, \pi]$ 、 $\phi \in [0, 2\pi]$ である。もとの基底空間Bの座標は (x, y) とし、 $x \in [0, W]$ 、 $y \in [0, H]$ とする。ここで、WとHは、画像の幅と高さである。このとき、 (θ, ϕ) と (x, y) とは簡単な座標変換によって相互に変換できる。この座標変換は、例えば、次式で与えられる。

【0073】

$$\theta = 2 \arctan [2 / |\tan^2 \{\pi/2(x/W-1/2)\} + \tan^2 \{\pi/2(y/H-1/2)\}|]$$

$$\cos \Phi = \tan^2 \{\pi/2(x/W-1/2)\} / |\tan^2 \{\pi/2(x/W-1/2)\} + \tan^2 \{\pi/2(y/H-1/2)\}|$$

$$|$$

$$\sin \Phi = \tan^2 \{\pi/2(y/H-1/2)\} / |\tan^2 \{\pi/2(x/W-1/2)\} + \tan^2 \{\pi/2(y/H-1/2)\}|$$

$$|$$

次に、画素の色としては濃淡を例にとる（画像として濃淡画像を例にとる）。従って、色空間Cは、輝度値だけの1次元領域 $C = [0, 256]$ であるとする。

【0074】

ここでは、一例として、 $6g$ 枚 (g は予め定められた整数) のフレームから得られる積空間 C^{6g} を考える。連続する $6g$ 枚のフレームについて、連続する g 枚のフレームごとに分割して、6つのグループを作る。最初のグループ (G_0) と次のグループ (G_1) において、基底空間 B の各点ごとに、グループ G_0 の輝度値の和から、グループ G_1 の輝度値の和を引く。これによって得られる値を X とする。残りのグループ G_2 と G_3 、 G_4 と G_5 についても、それぞれ、同様の処理を行う。これらによって得られる値を Y 、 Z とする。こうして、基底空間 B の各点ごとに、3つの値 X 、 Y 、 Z が得られる。この様子を、図7に示す。なお、このグルーピングの仕方は、一例であり、何番目のフレームが何番目のグループに属するかを予め定めておけば、他のグルーピング方法によってもちろん構わない（様々なバリエーションが可能である）。

【0075】

ここで、それら3つの値 X 、 Y 、 Z を、 X 成分、 Y 成分、 Z 成分とするように、空間 S （色空間 C の中に対象空間 T を包含する所定の部分空間 S ）を構成する。

【0076】

6つのグループにおいて、 B の各点ごとに g 個のフレームの輝度値の和をとつて得られるものを、 $f_0, f_1, f_2, f_3, f_4, f_5 : B \rightarrow [0, 256g]$ とすると、 X 成分、 Y 成分、 Z 成分は、それぞれ、 $f_0 - f_1, f_2 - f_3, f_4 - f_5$ で与えられる。 $f_0 - f_1, f_2 - f_3, f_4 - f_5$ を、輝度差分値と総称するものとする。

【0077】

空間 S の座標 (X, Y, Z) は、 $X \in [-256g, 256g]$ 、 $Y \in [-256g, 256g]$ 、 $Z \in [-256g, 256g]$ である（厳密には、 $[-255g, 255g]$ 内にある）。

【0078】

空間 S の中に、半径 ϵ の2次元球面 S^2 をとり、これを対象空間 T とする。

【0079】

対象空間 T 上の座標として H 、極座標 (Θ, Φ) をとる。 $\Theta \in [0, \pi]$ 、 $\Phi \in [0, 2\pi]$ とする。対象空間 T 上の (Θ, Φ) は、空間 S 内の (X, Y, Z)

) で表すと、

$$X = \sin\Theta \cdot \cos\Phi$$

$$Y = \sin\Theta \cdot \sin\Phi$$

$$Z = \cos\Theta$$

となる。

【0080】

6 g枚の画像から得られる輝度差分値の画像を考えると、基底空間Bの各点において、対象空間T中的一点が割り当てられていることになる。この様子を、図8に表す。

【0081】

このようにして、6 g枚の画像から得られる輝度差分値の画像は、 S^2 から S^2 への写像として定義される。

【0082】

この場合、電子透かしとして利用するホモトピー類は、2次元球面 $B = S^2$ から2次元球面 $T = S^2$ への写像の間のホモトピー同値に関する同値類 $\pi^2(S^2)$ である。 $\pi^2(S^2) = \mathbb{Z}$ であることが知られている。ここで、 \mathbb{Z} は、有理整数の集合である。また、 $=$ は、「群としての同型」を意味するものとする。よって、電子透かしは、整数値によって与えられる。そこで、このホモトピーハイツの元が透かし情報を表現するように、画像を変更することで、透かし情報の埋め込みを行うことが可能である。

【0083】

例えば、図6の画像の左上を原点にとると、ホモトピー類 $b = 1$ の場合には、該画像の外周（端部）が2次元球面の $(0, 0, 1)$ すなわち北極にあたる部分に対応し、該画像の中心が2次元球面の $(0, 0, -1)$ すなわち南極にあたる部分に対応し、その間は、連続的に対応することになる。すなわち、図6の基底空間での赤道周りでの1周が、図8の対象空間での赤道周りでの1周に対応する。

【0084】

この様子を、図9～図12に示す。各図において、(a) は画像上の位置のう

ち2次元球面の基底空間におけるある経線に対応する部分を両矢印で示し、(b)，(c)は(a)で示された部分に埋め込まれている値が示す対象空間における位置を示す。また、(b)は対象空間を北極側からみた様子を示し、(c)は対象空間を赤道側からみた様子を示している。

【0085】

なお、ホモトピー類 $b = -1$ の場合にも、同様であるが、対象空間での赤道周りでの1周が、 $b = 1$ の場合に比べて逆回りになる。また、 $b = 2$ または -2 の場合には、基底空間での赤道周りでの1周が、対象空間での赤道周りでの2周に対応する。

【0086】

本具体例では、各画素の輝度差分値が、上記のようにホモトピー類 b に応じた対応を与えるように、画素値の変更を行うことによって、ホモトピー類 b の埋め込みを行えばよい。

【0087】

ただし、詳しくは後述するが、本実施形態では、画像への電子透かしの埋め込みを行う前に、各画素へ埋め込むべき値に対する鍵情報に基づく搔き混ぜを行う。すなわち、図13に示すように、(a)のような画像の本来の各画素位置に、各埋め込み値を埋め込む前に、(b)のように搔き混ぜを行って、埋め込む。この状態では、同じアルゴリズムを用いても、基底空間での赤道周りでの1周が、対象空間ではランダムな遷移を示すだけであり、意味のある情報を得ることはできない(正しいホモトピー類すなわち電子透かしを求めることがないばかりでなく、電子透かしの存在自体が分からぬ)。埋め込み時に用いられた鍵情報に対応する鍵情報があつてはじめて、図14に示すように、搔き混ぜ戻しを行つて、画像の本来の各画素位置に対応する各埋め込み値を検出することができ、正しいホモトピー類すなわち電子透かしを求めることができる。

【0088】

このように、電子透かしのアルゴリズムが開示されたとしても鍵情報が開示されていなければ安全であるように構成することができるようとしている。

【0089】

図15に、本具体例の場合の電子透かし埋込装置における処理手順の一例を示す。

【0090】

まず、最初に、電子透かし埋込装置には、電子透かしを埋め込む対象となる埋め込み対象画像と、埋め込むべき透かし情報であるホモトピー類と、鍵情報とが与えられる。

【0091】

次に、関数生成部11は、与えられたホモトピー類に属する関数を生成する。

【0092】

関数生成部11の具体例を説明する。

【0093】

関数生成部11は、X成分生成部とY成分生成部とZ成分生成部とを含む（図示せず）。関数の形には、種々のバリエーションがあるが、一例として、次のようなものがある。

$$\Theta = \theta \quad (1)$$

$$\Phi = b \phi \quad (m \text{ o d } 2\pi) \quad (2)$$

ここで、bは、電子透かしであるのもトピー類であって、 $b \in \mathbb{Z} \oplus \pi^2 (S^2)$ である。

【0094】

なお、あるホモトピー類に属する関数として、上記式以外のものを選択してもよい。周期的ではない関数でもよい。

【0095】

また、予め用意された複数の異なる関数をそれぞれ用いてコンテンツに対する位相不变量の設定を行ったとした場合に対象コンテンツの内容に与える影響を評価し、対象コンテンツの内容に与える影響を最小にすると評価される関数を選択するようにしてもよい。

【0096】

ところで、対象空間T上の点に対応する座標(X, Y, Z)の値は、座標(Θ, Φ)の値の関数であり、上記式より、座標(Θ, Φ)の値は、基底空間Bと同

一覧された S^2 上の座標 (θ, ϕ) の値の関数である。基底空間 B 上の各点に対する (X, Y, Z) の値の計算は、この座標変換を表す式中に現れる初等的な関数を計算する機能を組み合わせて用いることで実現できる。初等的な関数の計算は、例えば、その関数の入力と出力の対応をテーブルとして持つことにより実現できる。

【0097】

こうして、関数生成部 1 1 は、電子透かし情報 $b \in ZZ$ の入力に対して、B の各点に対して、対応する (X, Y, Z) の値を出力する。

【0098】

次に、掻き混ぜ関数生成部 1 1 は、与えられた鍵情報に従って、掻き混ぜ関数を生成し、関数生成部 1 1 が生成した関数との合成関数を計算する。

【0099】

関数掻き混ぜ部 1 2 の具体例を説明する。

【0100】

関数掻き混ぜ部 1 2 は、鍵情報 k の入力に対して、掻き混ぜ関数を生成する。

【0101】

掻き混ぜ関数は、S から S への写像であって、鍵情報の値により異なる写像となるものである。

【0102】

以下、その一例を示す。

【0103】

空間 S の各座標を、それぞれ、256 のブロックに分割する。

【0104】

座標ごとにブロックを指定するためには、8 ビットあればよいので、3 つの座標 (X, Y, Z) のすべてでブロックを指定するには、24 ビットあればよい。この (X, Y, Z) を表す 24 ビットの情報が指定されると、空間 S 中のある一区画が特定される。ここでは、これらの区画の間の置換を鍵情報に依存して生成する。そのためには、24 ビットの情報が入力されると、24 ビットの情報を出力する全単射の関数を鍵依存となるように構成できればよい。このために、本例

では、ブロック暗号の構成方法を用いる。

【0105】

ブロック暗号の構成方法の1つがFeistel網を利用する方法であり、DESがその例である。

【0106】

ここでは、Feistel網を利用して図16に例示するような構成を用いる。

【0107】

図16中、121は、排他的論理和である。122の部分の内部構成において、1221はS-box、1222は排他的論理和である。S-boxは、8入力8出力の全単射関数で、ランダムな変換を行う。r回同じ操作を繰り返すことで、入力と出力は、ランダムな関係となる。k₁～k_rは、鍵情報である。この場合、鍵情報kは、k₁～k_rの合わせて8rビットの長さとなる。掛け混ぜ関数g_kは、この区間の置き換えとする。

【0108】

図16の構成の上部から、関数生成部11が生成した関数値が入力され、図16の構成の下部から、それが掛け混ぜ関数と合成された結果の関数値が出力される。

【0109】

関数掛け混ぜ部12は、関数生成部11から得た基底空間Bから対象空間Tへの関数 Ψ_b に対して、S \subset Tに対して、生成したSからSへの掛け混ぜ関数g_kを適用し、基底空間BからS内への関数g_k \bigcirc Ψ_b を生成する。これは、関数生成部11が与えられた基底空間Bの各点に対応する対象空間T上の点を、さらに、掛け混ぜ関数の対応関係に従って、S内の点に写すことによって行われる。

【0110】

なお、上記では、X成分とY成分とZ成分をまとめて同一の掛け混ぜ関数を適用したが、その代わりに、X成分とY成分とZ成分とに対して異なる掛け混ぜ関数を個別に適用するようにしてもよい。この場合には、後述する、掛け混ぜ戻しにおいては、X成分とY成分とZ成分とのそれぞれについて当該掛け混ぜ関数に

対応する搔き混ぜ戻し関数を個別に適用することになる。

【0111】

次に、合成関数のX成分、Y成分、Z成分の各成分は、それぞれ、 g 個のフレームからなるグループ2つに対して埋め込まれる。最後に、電子透かしが埋め込まれた埋め込み済み画像が出力される。

【0112】

関数埋め込み部13の具体例を説明する。

【0113】

関数埋め込み部13は、関数搔き混ぜ部12が出力した合成関数 $g_k \bigcirc \Psi_b : B \rightarrow S$ を埋め込み対象画像に埋め込む。

【0114】

前述したように、6枚のフレームを6つのグループ $G_0 \sim G_5$ に分け、X成分、Y成分、Z成分に対応する2つのグループ G_0 と G_1 , G_2 と G_3 , G_4 と G_5 に対して、それぞれ、次のように、合成関数のX成分、Y成分、Z成分の埋め込みを行う。

[X成分]

$$\text{グループ } G_0 : f_0 \rightarrow f_0 + (\epsilon/2) [g_k \bigcirc \Psi_b]_x$$

$$\text{グループ } G_1 : f_1 \rightarrow f_1 - (\epsilon/2) [g_k \bigcirc \Psi_b]_x$$

[Y成分]

$$\text{グループ } G_2 : f_2 \rightarrow f_2 + (\epsilon/2) [g_k \bigcirc \Psi_b]_y$$

$$\text{グループ } G_3 : f_3 \rightarrow f_3 - (\epsilon/2) [g_k \bigcirc \Psi_b]_y$$

[Z成分]

$$\text{グループ } G_4 : f_4 \rightarrow f_4 + (\epsilon/2) [g_k \bigcirc \Psi_b]_z$$

$$\text{グループ } G_5 : f_5 \rightarrow f_5 - (\epsilon/2) [g_k \bigcirc \Psi_b]_z$$

例えば、X成分について、埋め込み前に検出されるグループ G_0 の輝度差分値が f_0 であったならば、埋め込み後に検出されることになる輝度差分値が $f_0 + (\epsilon/2) [g_k \bigcirc \Psi_b]_x$ となるように、各フレームの画素の画素値を変更することによって、埋め込みを行う。

【0115】

なお、各 f_i への埋め込みは、そのグループに属する g 枚のフレームに対して均等に埋め込みを行ってもよいし、フレーム毎に、埋め込む強さを変えてよい。さらに、均等に埋め込むか、埋め込む強さを変えるかを、B の点毎に、決めてよい。また、フレーム毎の埋め込む強さの変え方も B の点毎に変えてよい。

【0116】

また、実際に透かし情報の埋め込みに用いるのは、画素値の全ビットではなく、そのうち、ノイズの影響を受けにくく、かつ、画像の画質に大きな影響を与えない、予め定められた特定の中間のビットプレーンの領域（通常は連続する複数ビット）を用いるようにしてもよい。

【0117】

図17に、本具体例の場合の電子透かし検出装置における処理手順の一例を示す。

【0118】

まず、最初に、電子透かし検出装置には、電子透かしを検出する対象となる検出対象画像と、電子透かしの埋め込みに用いられた鍵情報が与えられる。

【0119】

次に、関数検出部21は、埋め込まれている関数のX成分、Y成分、Z成分をそれぞれ g 個のフレームからなる2つのグループから抽出する。

【0120】

関数検出部21の具体例を説明する。

【0121】

関数検出部21は、 $6g$ 個のフレームから、図7のように、X成分、Y成分、Z成分を計算する。なお、埋め込みの際には、 ϵ という定数を掛けて埋め込んでいたので、検出の際には、検出された成分値に $1/\epsilon$ を掛けておく。

【0122】

こうして、関数 $\Phi : B \rightarrow S$ が求まる。

【0123】

関数の表現方法の例としては、基底空間 B の点ごとに、関数値を対応付けたりストとして表す方法がある。

【0124】

次に、関数掻き混ぜ戻し部22は、与えられた鍵情報に従って、掻き混ぜ戻し関数を生成し、関数検出部21が抽出した関数との合成関数を計算する。

【0125】

関数掻き混ぜ戻し部22は、与えられた鍵情報kに従って、掻き混ぜ戻し関数を生成する。この掻き混ぜ戻し関数は、埋め込みの際に用いた鍵と同じ鍵が与えられた場合には、掻き混ぜ関数の逆関数となっている。

【0126】

関数掻き混ぜ部12においては、Festel網を利用して図16のような構成で掻き混ぜ関数を実現したが、その逆関数は、図18に例示するような構成で実現できる。

【0127】

図18中、221は、排他的論理和である。222の部分の内部構成において、2221はS-box、2222は排他的論理和である。k₁～k_rは、鍵情報である。

【0128】

図18の構成の上部から、関数検出部21が抽出した関数値が入力され、図18の構成の下部から、それが掻き混ぜ戻し関数と合成された結果の関数値が出力される。

【0129】

次に、ホモトピー類計算部23は、得られた合成関数から、ホモトピー類を計算する。最後に、計算されたホモトピー類が電子透かしとして出力される。

【0130】

ホモトピー類計算部2は、関数掻き混ぜ戻し部22によって計算された合成関数から、ホモトピー類を計算する。

【0131】

関数掻き混ぜ戻し部22の計算した合成関数を、

$ff = (X, Y, Z) = (\sin\Theta \cdot \cos\Phi, \sin\Theta \cdot \sin\Phi, \cos\Theta)$
で表す。

【0132】

関数搔き混ぜ戻し部22に埋め込みの際に用いた鍵と同じ鍵が与えられた場合には、この合成関数は、電子透かし埋込装置の関数生成部11が生成した、電子透かしとして与えられたホモトピー類bに属する関数 ($\Psi_b : B \rightarrow T$) である。

【0133】

この合成関数のホモトピー類b (ff) は、

$$b(ff) = (1/4\pi) \int_0^{2\pi} d\theta \int_0^\pi d\phi \, ff \cdot \partial ff / \partial \theta \times \partial ff / \partial \phi$$

で計算される。ここで、 θ, ϕ は、基底空間Bと同一視された2次元球面 S^2 上の座標である。また、ベクトル演算において、 \cdot と \times は、それぞれ、X座標、Y座標、Z座標を正規直交するとみなしたときの、空間S内の内積と外積である。なお、 $\int_0^{2\pi}$ の0と 2π は積分の範囲が $0 \sim 2\pi$ であることを示している。

【0134】

もとの基底空間B上の積分で表すと、ホモトピー類b (ff) は、

$$b(ff) = (1/4\pi) \int_0^W d\theta \int_0^H dy \, ff \cdot \partial ff / \partial x \times \partial ff / \partial y$$

となる。

【0135】

実際の画像において、Bは離散空間であるから、上記式における積分は和によって置き換えられ、微分は差分によって置き換えて行われる。この場合、ホモトピー類b (ff) は、

$$b(ff) = (1/4\pi WH) \sum_{x=0}^{W-1} \sum_{y=0}^{H-1} ff \cdot \Delta_x ff \times \Delta_y ff \quad (3)$$

となる。

【0136】

ここで、

$$\Delta_x ff(x, y) = ff(x+1, y) - ff(x, y) \quad (x \neq W-1 のとき)$$

$$\Delta_x ff(x, y) = ff(0, y) - ff(W-1, y) \quad (x = W-1 のとき)$$

$$\Delta_y ff(x, y) = ff(x, y+1) - ff(x, y) \quad (x \neq H-1 のとき)$$

$$\Delta_y ff(x, y) = ff(x, 0) - ff(x, H-1) \quad (x = H-1 のとき)$$

である。

なお、 $\sum_{x=0}^{W-1}$ の $x=0$ と $W-1$ は総和の範囲が $x=0 \sim W-1$ であることを示している。

【0137】

最終的には、この計算結果に最も近い整数値を電子透かしの値として出力する。

【0138】

図19に、ホモトピー類計算部23の構成例を示す。

【0139】

第1の微分計算部231は、上記のx方向の微分（差分）を計算し、第2の微分計算部232は、上記のy方向の微分（差分）を計算する。外積計算部233は、これら2つの微分（差分）の外積を計算し、内積計算部234は、この内積結果と、もとの関数を内積する。最後に、積分計算部235は、この内積結果を基底空間Bに渡って積分し、必要に応じて、整数値への丸めを行う。

【0140】

ところで、上記具体例では、6g枚のフレームをもとに処理を行ったが、例えば、4つのフレームを縦横に接続してこれを処理上の1フレームとみなして処理する方法（この場合、24g枚のフレームをもとに処理することになる）や、1つのフレームを縦横に分割してこれを処理上の4つの連続するフレームとみなして処理する方法（この場合、6g/4枚のフレームをもとに処理することになる）なども可能である。

【0141】

また、上記具体例では、濃淡画像を例にとって説明したが、本実施形態は、もちろん、カラー画像にも適用可能である。この場合には、例えば、最初のg枚の画素の色のY成分をグループG₀、次のg枚の画素の色のY成分をグループG₁、最初のg枚の画素の色のU成分をグループG₂、次のg枚の画素の色のU成分をグループG₃、最初のg枚の画素の色のV成分をグループG₄、次のg枚の画素の色のV成分をグループG₅として、同様の処理を行えばよい。また、Y成分のみを用いるものとして、同様の処理を行うことも可能である。その他にも、種々のバリエーションが可能である。もちろん、カラー画像においても、何番目のフレームのどの成分が何番目のグループに属するかを予め定めておけば、どのようなグルーピングの仕方によっても構わない（様々なバリエーションが可能である）

。

【0142】

また、上記具体例では、動画像を例にとって説明したが、本実施形態は、静止画にも適用可能である。この場合には、例えば、静止画を6g個に分割して、分割部分のそれぞれを処理上の1フレームとみなして処理するようにしてもよい。

【0143】

また、上記具体例では、隣接する2つの（例えばg枚の画素からなる）グループの画素値に関する差分値を利用して、電子透かしを埋め込むようにしたが、1つの（例えばg枚の画素からなる）グループに直接電子透かしを埋め込など、種々の方法が可能である。

【0144】

また、これまで本実施形態で説明した埋め込み方は、一例であり、他の異なる埋め込み方法も可能である。

【0145】

以下では、本実施形態のさらなるバリエーションについて詳しく説明する。

【0146】

まず、これまで各構成例では、基底空間をS²、対象空間をS²として説明したが、それぞれ、非自明なトポロジーを持つ基底空間や対象空間を用いる場合など、他の空間を採用することによる実現形態も可能である。

【0147】

例えば、画像の上端と下端とを同一視し、右端と左端とを同一視することで、基底空間をトーラスT²とすることも可能である。

【0148】

次に、埋め込み画像を表す関数のバリエーションについて説明する。

【0149】

埋め込み画像を表す関数において、画像周辺近傍での関数の変化を緩やかにし、周辺に近づくにつれ一定の値に漸近的に近づくように取れば、画像の切り取りが画像の中央付近の切り取りである場合には、失われた周辺部の積分値への影響は小さい。したがって、画像の中央付近に重要な内容が集中したコンテンツの場

合には（そのようなコンテンツは比較的多いと考えられる）、切り取りに対する耐性もある程度実現できる。一般的には、その画像の重要な部分において関数の変化が大きくなるようすれば、重要な部分だけを切り抜いても電子透かしが残るようになる。

【0150】

次に、音声データに対する処理のバリエーションについて説明する。

【0151】

これまで、対象コンテンツとして画像を例にとって説明してきたが、本実施形態は、他のメディアのデジタルコンテンツに対しても適用可能である。例えば、音声や音楽のデジタルコンテンツについては、特開2002-142094に開示された方法を用いればよい。

【0152】

次に、位相不变量のバリエーションについて説明する。

【0153】

本実施形態では、位相不变量としてホモトピー類を用いて説明してきたが、それ以外の位相不变量を用いることも可能である。

【0154】

ホモトピー群（の元）以外の不变量（invariant）としては、例えば、ホモロジー群、コホモロジー群、あるいは、ベクトル束におけるStiefel-Whitney類、Chern類、Pontryagin類といった特性類（characteristic class）、多様体のEuler数、指数（index）や符号数（signature）、結び糸に関するAlexander不变量、あるいは、絡み糸に関するMilnor不变量など、多数のものが知られており（例えば、岩波数学事典第3版、日本数学会編集、岩波書店）、それら不变量を用いることも可能である。

【0155】

なお、ホモトピー群では、例えば、Gauss-Bonnetの定理によって与えられる積分を用いたが、Chern類などの特性類の場合には、例えば、Atiyah-Singerの指数定理が与える積分を用いることができる。それ

らの場合、ホモトピー群について例示した積分量の代わりに、それらの不变量を導き出す積分量を用いればよい。

【0156】

以下では、本実施形態のハードウェア構成、ソフトウェア構成について説明する。

【0157】

本実施形態の電子透かし埋込装置は、ハードウェアとしても、ソフトウェア（コンピュータに所定の手段を実行させるための、あるいはコンピュータを所定の手段として機能させるための、あるいはコンピュータに所定の機能を実現させるための）プログラム）としても、実現可能である。また、電子透かし埋込装置をソフトウェアで実現する場合には、記録媒体によってプログラムを受け渡しすることも、通信媒体によってプログラムを受け渡しすることもできる。もちろん、それらは、電子透かし検出装置についても同様である。

また、電子透かし埋込装置や電子透かし検出装置をハードウェアとして構成する場合、半導体装置として形成することができる。

また、本発明を適用した電子透かし埋込装置を構成する場合、あるいは電子透かし埋め込みプログラムを作成する場合に、同一構成を有するブロックもしくはモジュールがあっても、それらをすべて個別に作成することも可能であるが、同一構成を有するブロックもしくはモジュールについては1または適當数のみ用意しておいて、それをアルゴリズムの各部分で共有する（使い回す）ことも可能である。電子透かし検出装置を構成する場合、あるいは電子透かし検出プログラムを作成する場合も、同様である。また、電子透かし埋込装置および電子透かし検出装置を含むシステムを構成する場合、あるいは電子透かし埋め込みプログラムおよび電子透かし検出プログラムを含むシステムを作成する場合には、電子透かし埋込装置（あるいはプログラム）と電子透かし検出装置（あるいはプログラム）に渡って、同一構成を有するブロックもしくはモジュールについては1または適當数のみ用意しておいて、それをアルゴリズムの各部分で共有する（使い回す）ことも可能である。

【0158】

また、電子透かし埋込装置や電子透かし検出装置をソフトウェアで構成する場合には、マルチプロセッサを利用し、並列処理を行って、処理を高速化することも可能である。

【0159】

なお、この発明の実施の形態で例示した構成は一例であって、それ以外の構成を排除する趣旨のものではなく、例示した構成の一部を他のもので置き換えたり、例示した構成の一部を省いたり、例示した構成に別の機能あるいは要素を付加したり、それらを組み合わせたりすることなどによって得られる別の構成も可能である。また、例示した構成と論理的に等価な別の構成、例示した構成と論理的に等価な部分を含む別の構成、例示した構成の要部と論理的に等価な別の構成なども可能である。また、例示した構成と同一もしくは類似の目的を達成する別の構成、例示した構成と同一もしくは類似の効果を奏する別の構成なども可能である。

また、この発明の実施の形態で例示した各種構成部分についての各種バリエーションは、適宜組み合わせて実施することが可能である。

また、この発明の実施の形態は、個別装置としての発明、関連を持つ2以上の装置についての発明、システム全体としての発明、個別装置内部の構成部分についての発明、またはそれらに対応する方法の発明等、種々の観点、段階、概念またはカテゴリに係る発明を包含・内在するものである。

従って、この発明の実施の形態に開示した内容からは、例示した構成に限定されることなく発明を抽出することができるものである。

【0160】

本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【0161】

【発明の効果】

本発明によれば、S t i r M a r k 攻撃やD-A-D-変換などの局所的変形に対する耐性を持つとともに、電子透かしのアルゴリズムの全部又は一部が開示されたとしてもなお安全であるような電子透かしを実現することができる。

【図面の簡単な説明】

【図 1】 本発明の一実施形態に係る電子透かし埋込装置及び電子透かし検出装置を含むコンテンツ流通システムの概略構成を示す図

【図 2】 同実施形態に係る電子透かし埋込装置の構成例を示す図

【図 3】 同実施形態に係る電子透かし埋込装置の処理手順の一例を示すフローチャート

【図 4】 同実施形態に係る電子透かし検出装置の構成例を示す図

【図 5】 同実施形態に係る電子透かし検出装置の処理手順の一例を示すフローチャート

【図 6】 同実施形態において基底空間を2次元球面と同一視する様子を説明するための図

【図 7】 同実施形態において動画像を対象コンテンツとする場合の輝度差分値の計算方法の一例を説明するための図

【図 8】 同実施形態における基底空間と対象空間との例を示す図

【図 9】 同実施形態における基底空間での赤道周りでの1周と対象空間での赤道周りでの1周との対応を説明するための図

【図 10】 同実施形態における基底空間での赤道周りでの1周と対象空間での赤道周りでの1周との対応を説明するための図

【図 11】 同実施形態における基底空間での赤道周りでの1周と対象空間での赤道周りでの1周との対応を説明するための図

【図 12】 同実施形態における基底空間での赤道周りでの1周と対象空間での赤道周りでの1周との対応を説明するための図

【図 13】 同実施形態における鍵情報に基づく掻き混ぜについて説明するための図

【図 14】 同実施形態における鍵情報に基づく掻き混ぜ戻しについて説明するための図

【図 15】 同実施形態に係る電子透かし埋込装置の処理手順の一例を示すフローチャート

【図 16】 同実施形態に係る関数掻き混ぜ部の構成例を示す図

【図17】 同実施形態に係る電子透かし検出装置の処理手順の一例を示す
フローチャート

【図18】 同実施形態に係る関数挿き混ぜ戻し部の構成例を示す図

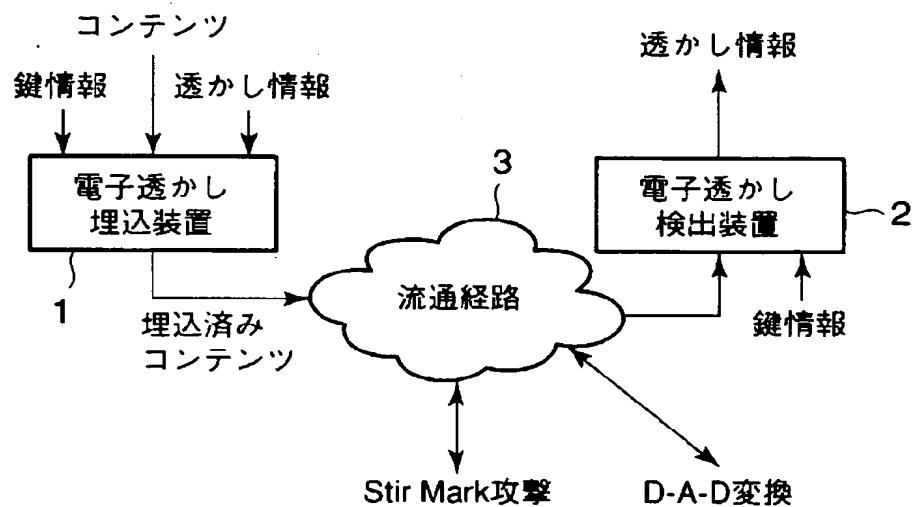
【図19】 同実施形態に係るホモトピー類計算部の構成例を示す図

【符号の説明】

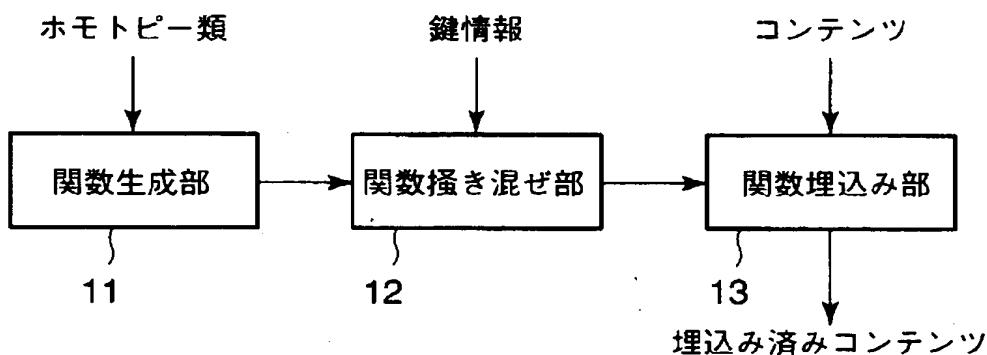
1…電子透かし埋込装置、 2…電子透かし検出装置、 3…流通経路、 1 1…関
数生成部、 1 2…関数挿き混ぜ部、 1 3…関数埋め込み部、 2 1…関数検出部、
2 2…関数挿き混ぜ戻し部、 2 3…ホモトピー類計算部、 1 2 1, 1 2 2 2, 2
2 1, 2 2 2 2…排他的論理和、 1 2 2 1, 2 2 2 1…S-box、 2 3 1…第
1の微分計算部、 2 3 2…第2の微分計算部、 2 3 3…外積計算部、 2 3 4…内
積計算部、 2 3 5…積分計算部

【書類名】 図面

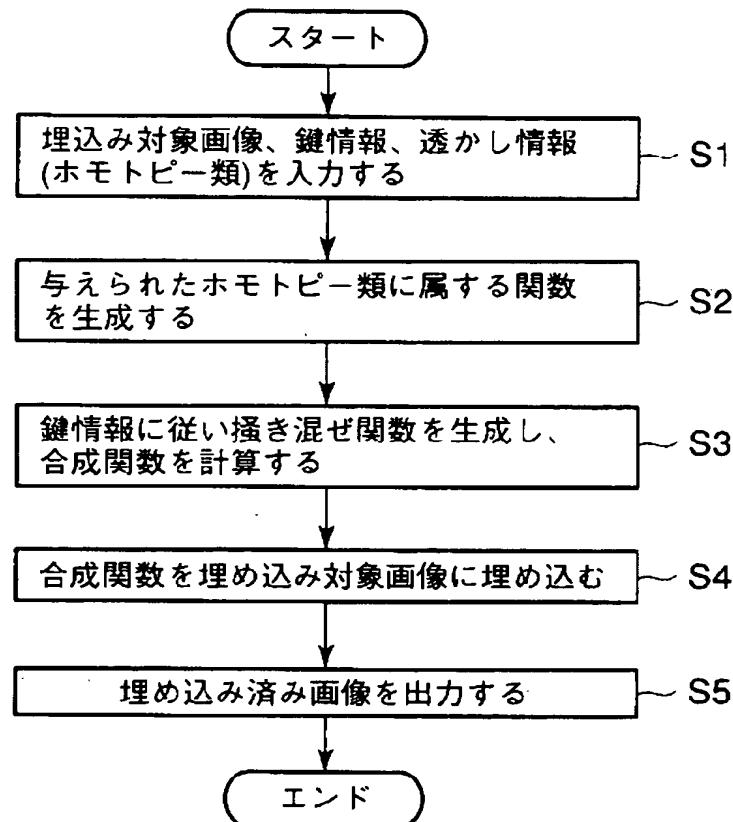
【図 1】



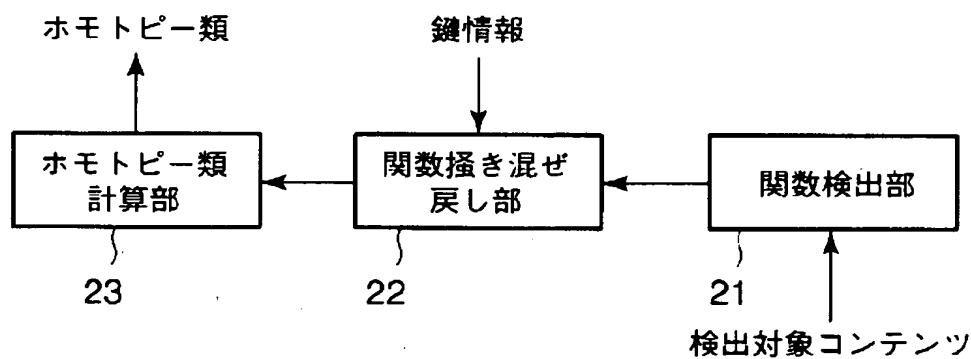
【図 2】



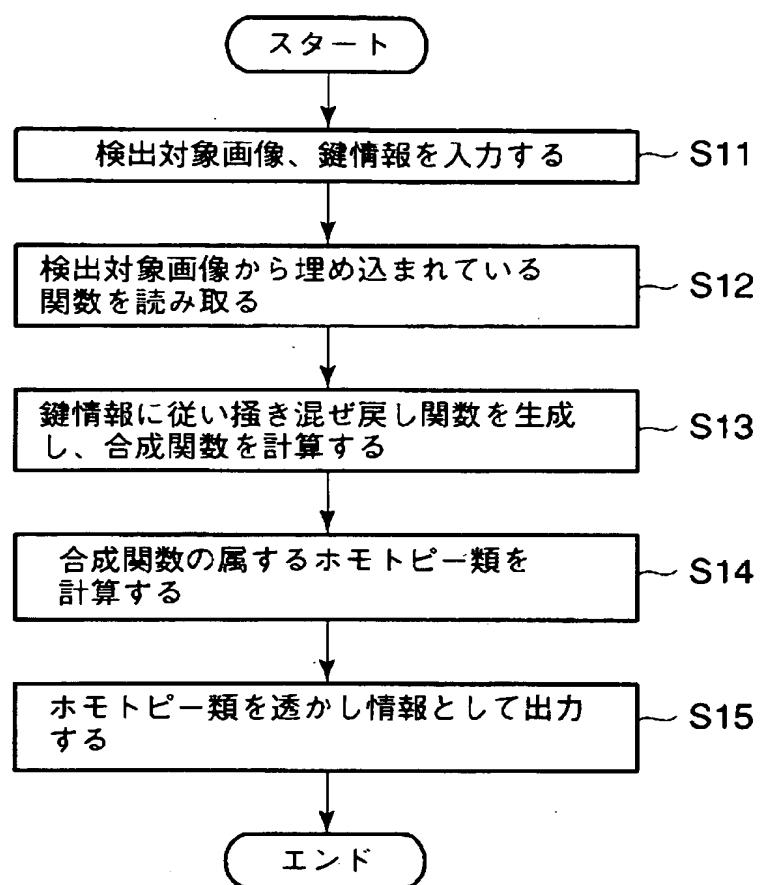
【図 3】



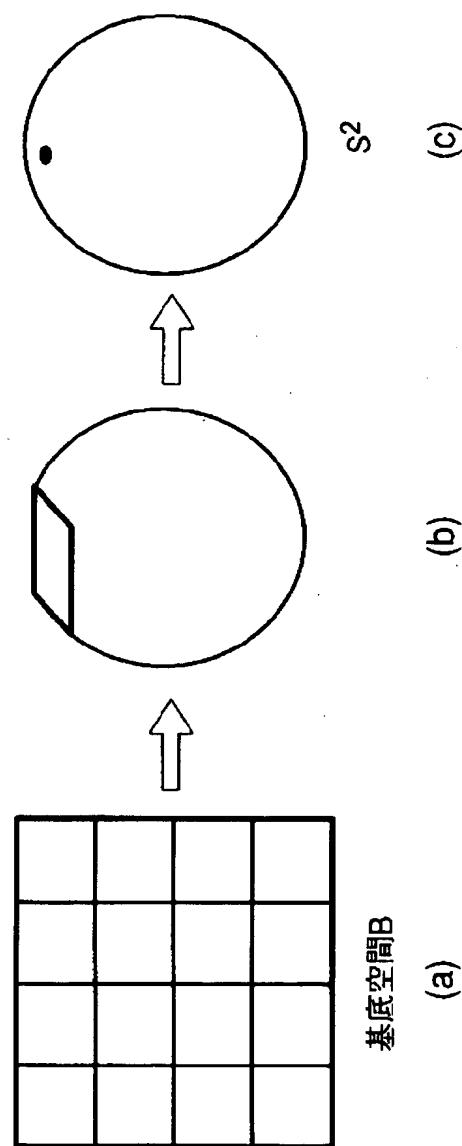
【図 4】



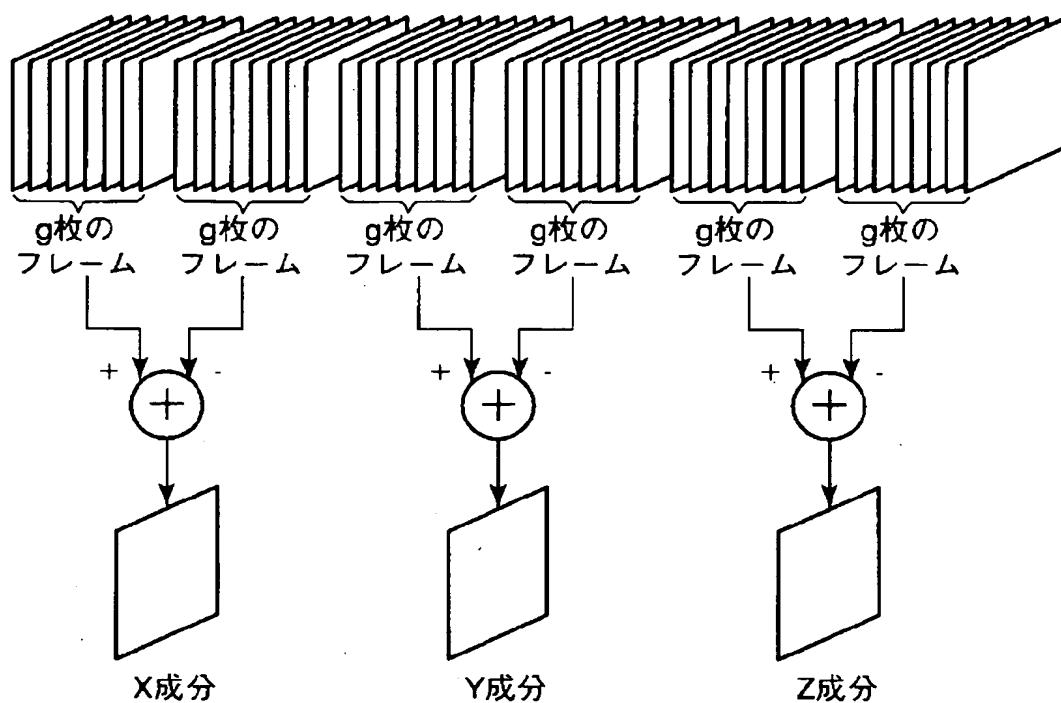
【図5】



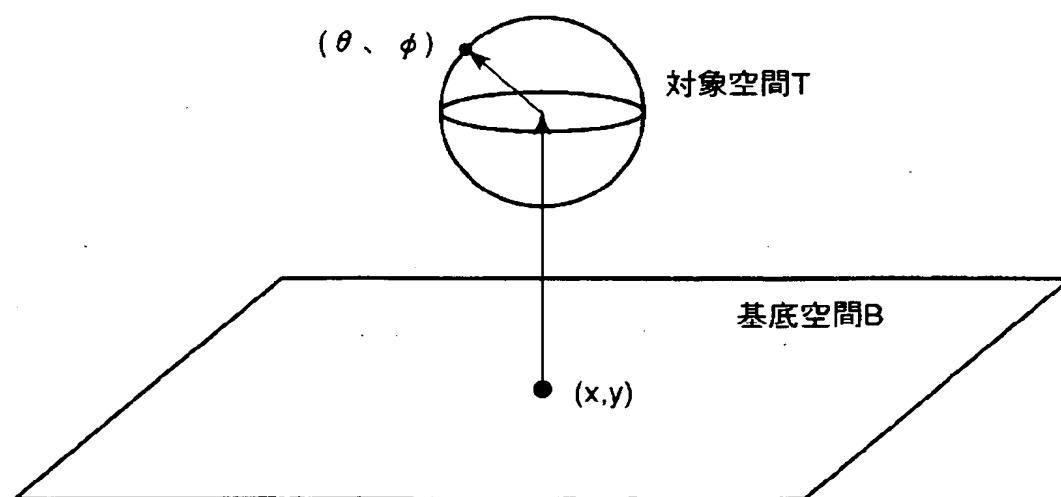
【図6】



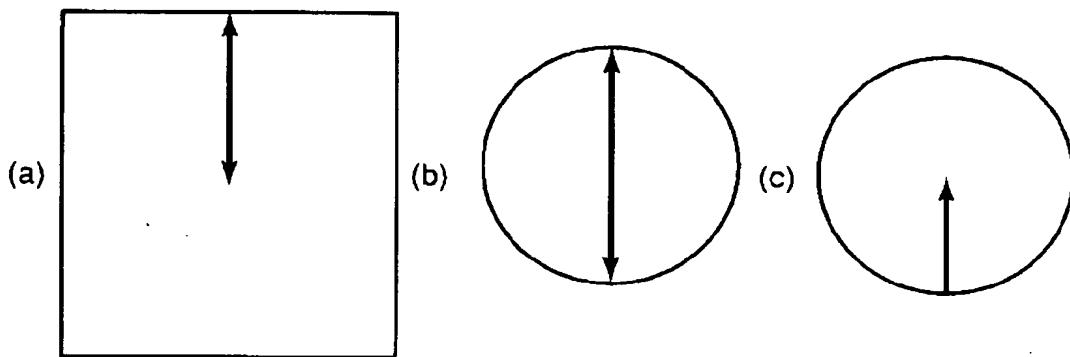
【図7】



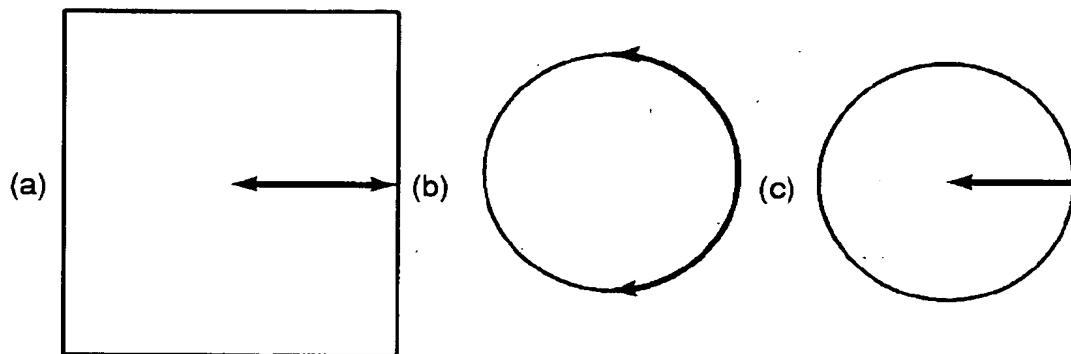
【図8】



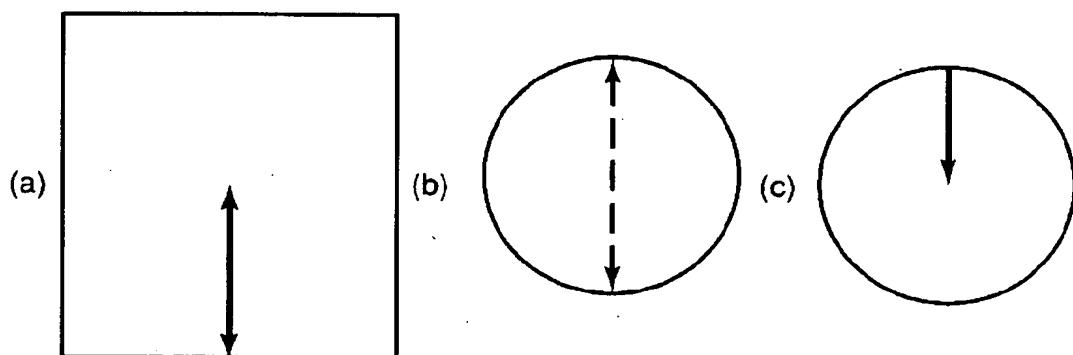
【図9】



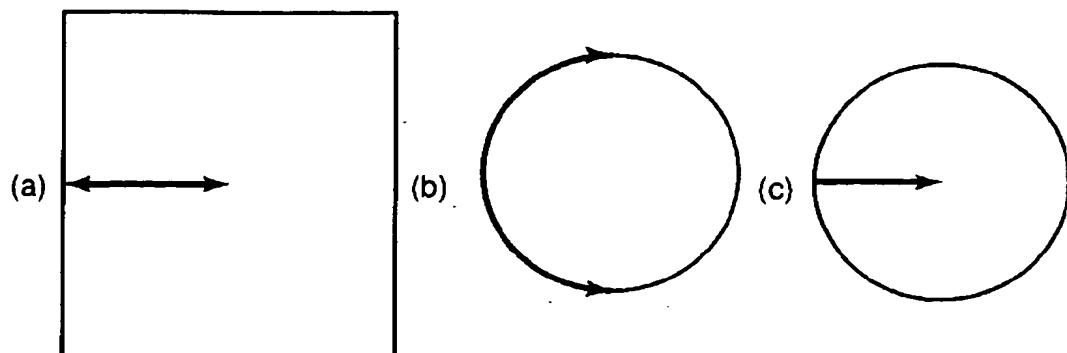
【図10】



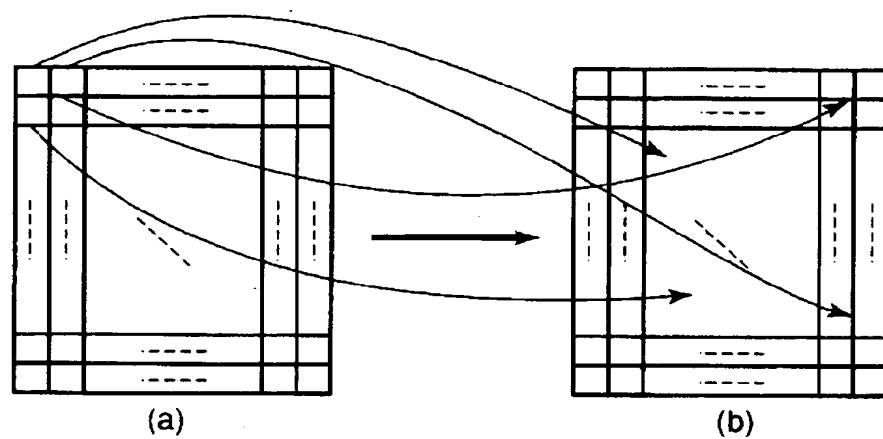
【図11】



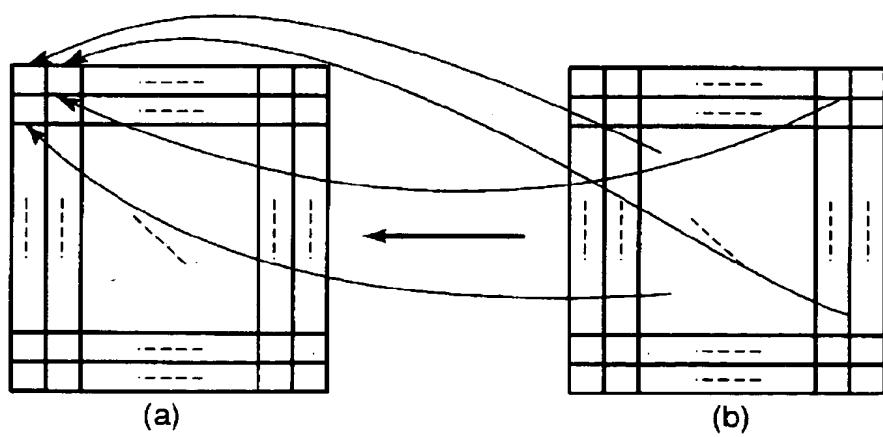
【図 1 2】



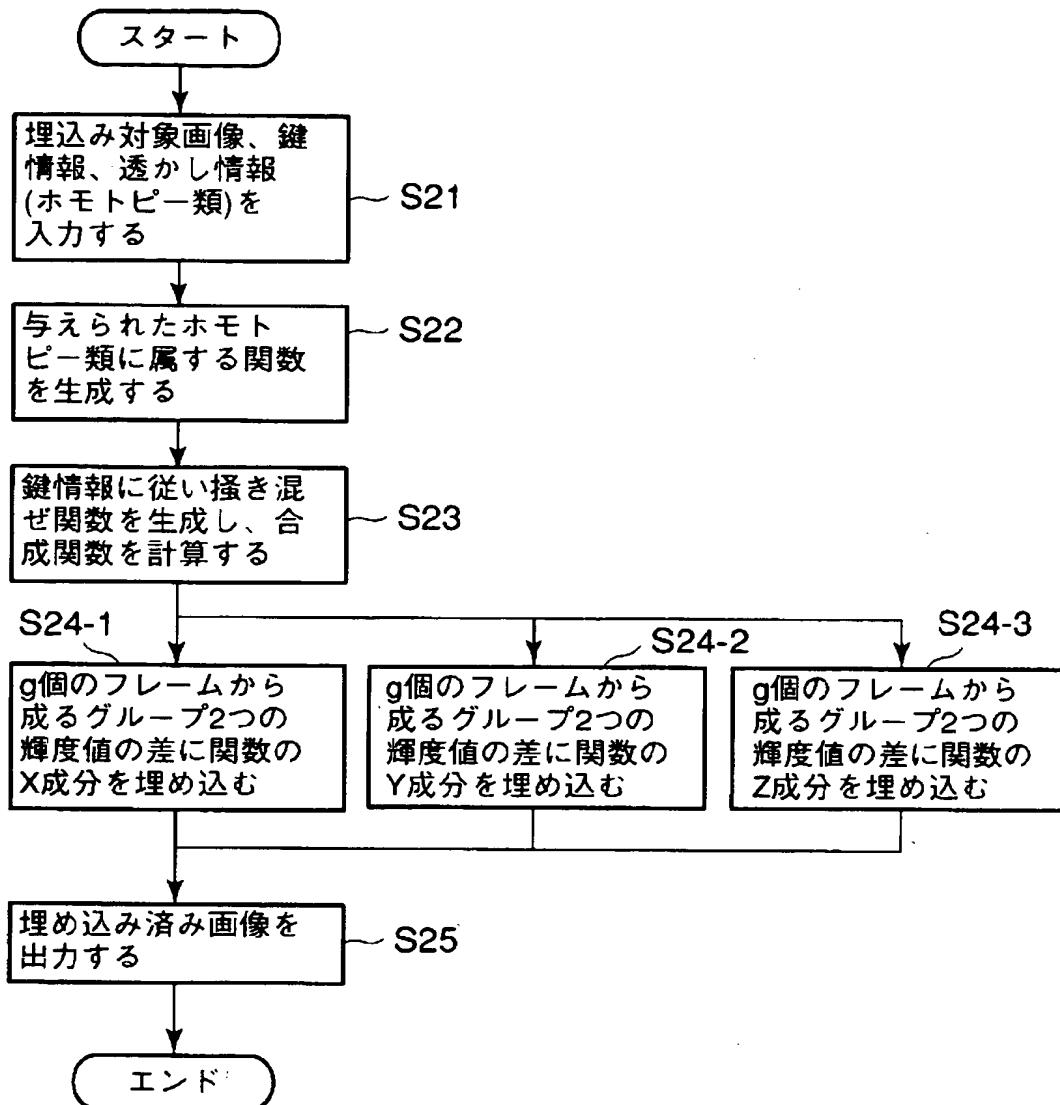
【図 1 3】



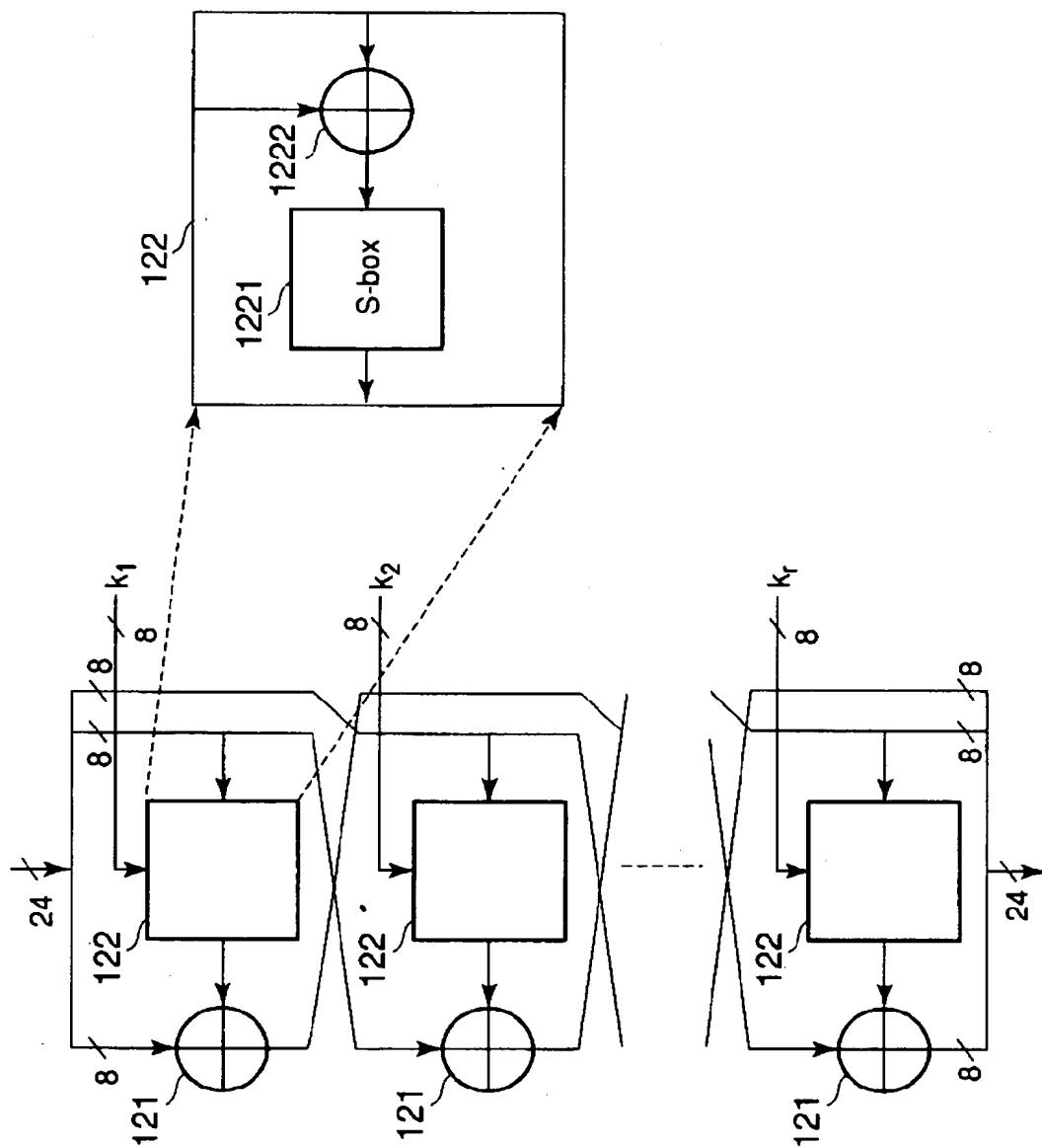
【図 1 4】



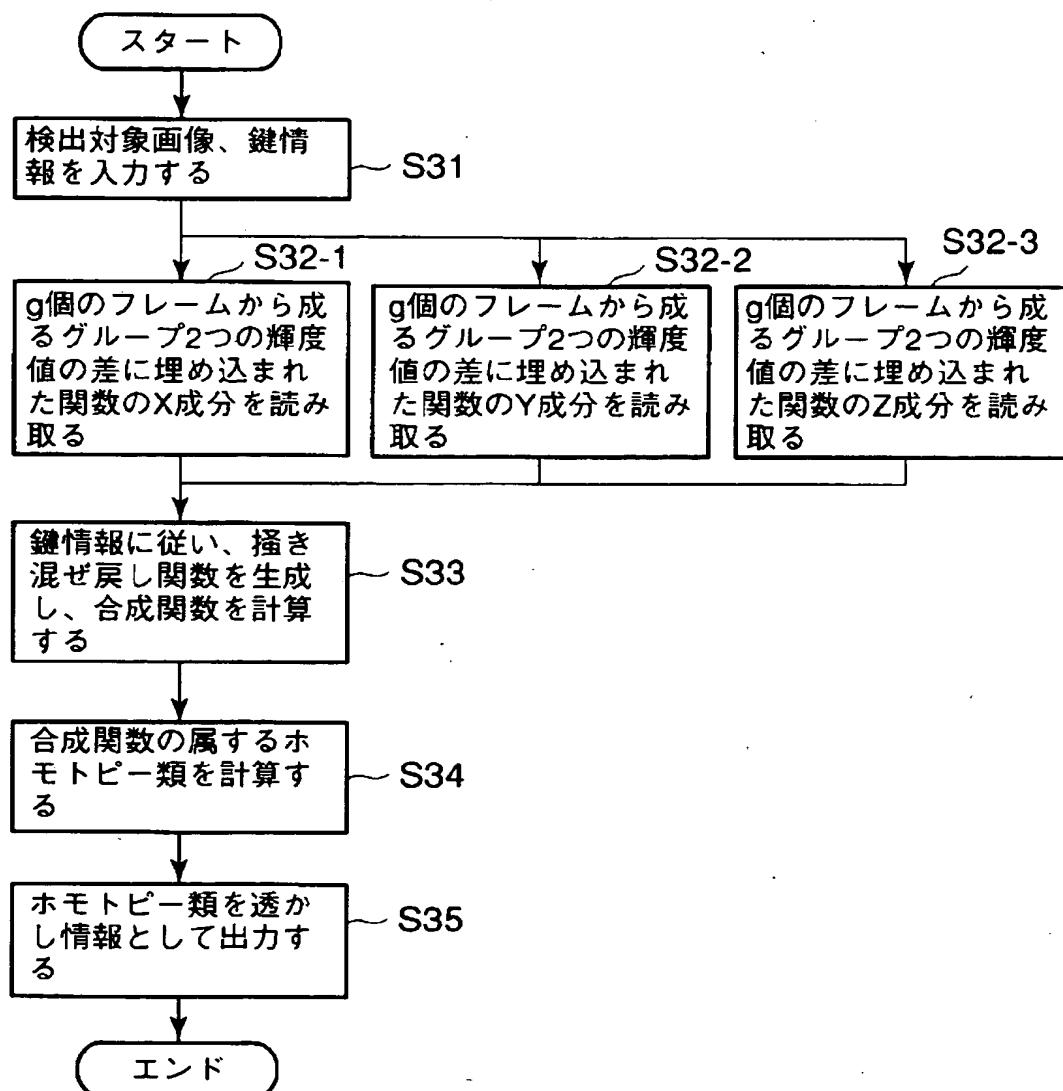
【図15】



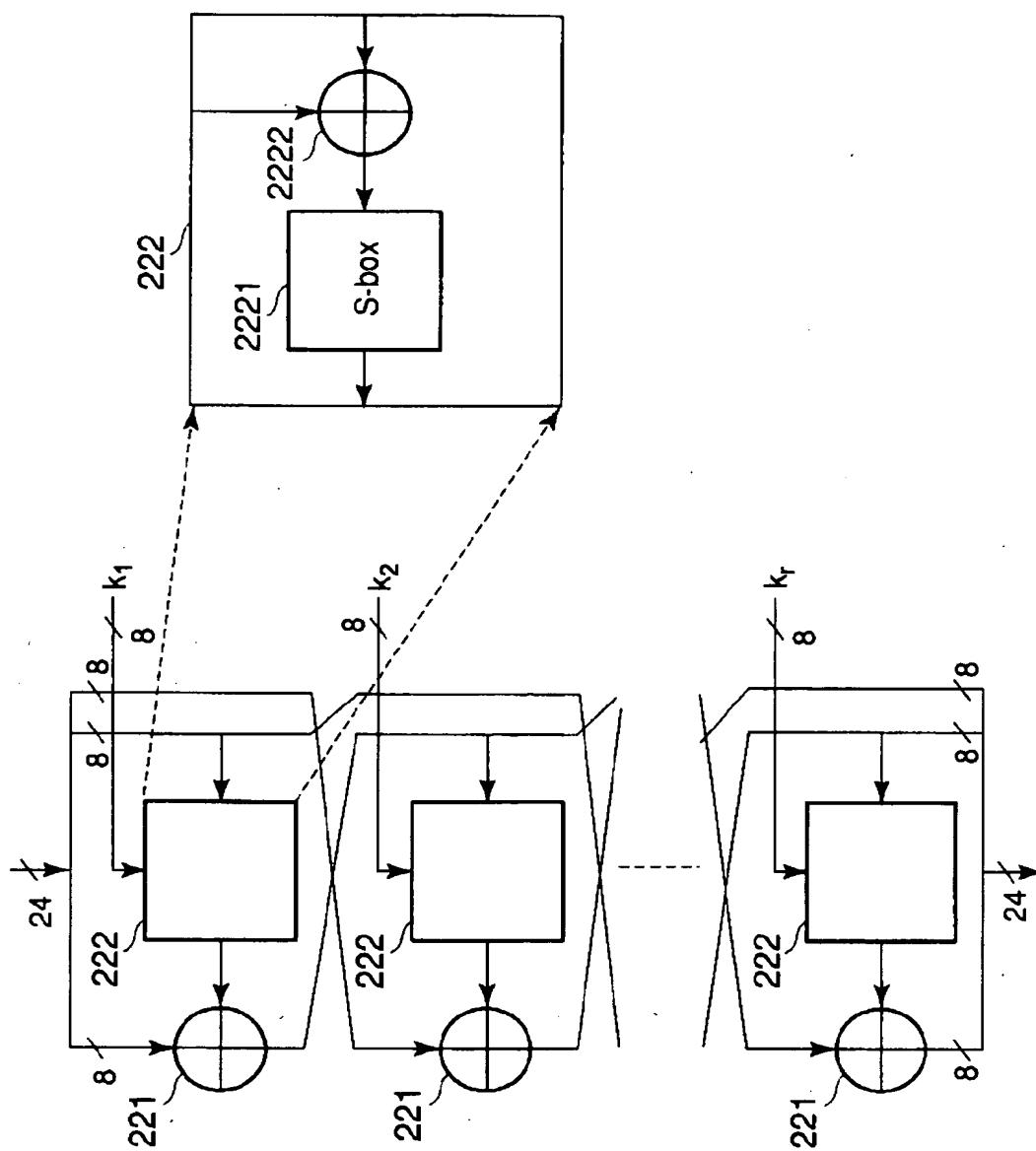
【図16】



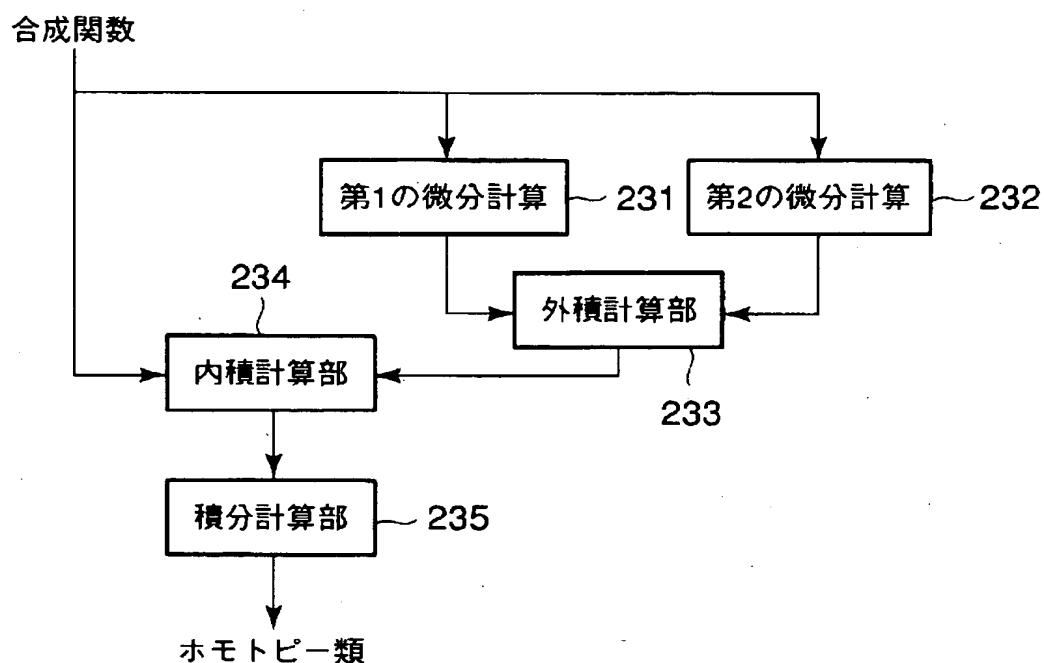
【図17】



【図18】



【図19】



【書類名】 要約書

【要約】

【課題】 StirMark攻撃やD-A-D-変換などの局所的変形に対する耐性を持つとともに、電子透かしのアルゴリズムの全部又は一部が開示されたとしてもなお安全であるような電子透かしシステムを提供すること。

【解決手段】 コンテンツに透かし情報を埋め込む電子透かし埋込装置1は、埋め込むべき位相不変量を入力し、コンテンツの内容のうち透かし情報の埋め込みに供される部分を変更することによって、コンテンツに位相不変量を設定する。その際、埋め込みに先立って、鍵情報に基づく搔き混ぜを行っておく。透かし情報を埋め込まれたコンテンツは流通経路3を流通する。コンテンツから透かし情報を検出する電子透かし検出装置2は、コンテンツの内容のうち予め定められた部分に基づいて、コンテンツに設定された位相不変量を検出する。その際、検出に先立って、正しい鍵情報に基づく搔き混ぜ戻しを行っておく必要がある。

【選択図】 図1

特願2002-381380

出願人履歴情報

識別番号 [000003078]

1. 変更年月日 2001年 7月 2日
[変更理由] 住所変更
住 所 東京都港区芝浦一丁目1番1号
氏 名 株式会社東芝

2. 変更年月日 2003年 5月 9日
[変更理由] 名称変更
住 所 住所変更
氏 名 東京都港区芝浦一丁目1番1号
株式会社東芝